electronics

MDPI

Article

DeepKnuckle: Deep Learning for Finger Knuckle Print Recognition

Ahmad S. Tarawneh [1], Ahmad B. Hassanat [2], Esra'a Alkafaween [2], Bayan Sarayrah [2], Sami Mnasri [3], Ghada A. Altarawneh [4], Malek Alrashidi [3], Mansoor Alghamdi [3] and Abdullah Almuhaimeed [5,*]

[1] Faculty of Informatics, Eotvos Lorand University, 1117 Budapest, Hungary; Ahmadtr@caesar.elte.hu
[2] Faculty of Information Technology, Mutah University, Mutah, Karak 6171, Jordan; hasanat@Mutah.edu.jo (A.B.H.); esrakafaween86@gmail.com (E.A.); Bayan.91@yahoo.com (B.S.)
[3] Department of Computer Science, Applied College, University of Tabuk, Tabuk 71491, Saudi Arabia; smnasri@ut.edu.sa (S.M.); Mqalrashidi@ut.edu.sa (M.A.); malghamdi@ut.edu.sa (M.A.)
[4] Department of Accounting, Mutah University, Mutah, Karak 6171, Jordan; Ghadaa@Mutah.edu.jo
[5] The National Centre for Genomics and Bioinformatics, King Abdulaziz City for Science and Technology, Riyadh 11442, Saudi Arabia
* Correspondence: muhaimed@kacst.edu.sa

Abstract: Biometric technology has received a lot of attention in recent years. One of the most prevalent biometric traits is the finger-knuckle print (FKP). Because the dorsal region of the finger is not exposed to surfaces, FKP would be a dependable and trustworthy biometric. We provide an FKP framework that uses the VGG-19 deep learning model to extract deep features from FKP images in this paper. The deep features are collected from the VGG-19 model's fully connected layer 6 (F6) and fully connected layer 7 (F7). After applying multiple preprocessing steps, such as combining features from different layers and performing dimensionality reduction using principal component analysis (PCA), the extracted deep features are put to the test. The proposed system's performance is assessed using experiments on the Delhi Finger Knuckle Dataset employing a variety of common classifiers. The best identification result was obtained when the Artificial neural network (ANN) classifier was applied to the principal components of the averaged feature vector of F6 and F7 deep features, with 95% of the data variance preserved. The findings also demonstrate the feasibility of employing these deep features in an FKP recognition system.

Keywords: biometrics; transfer learning; finger-knuckle print recognition; deep learning; VGG-19; PCA

check for updates

Citation: Tarawneh, A.S.; Hassanat, A.B.; Alkafaween, E.; Sarayrah, B.; Mnasri, S.; Altarawneh, G.A.; Alrashidi, M.; Alghamdi, M.; Almuhaimeed, A. DeepKnuckle: Deep Learning for Finger Knuckle Print Recognition. *Electronics* **2022**, *11*, 513. https://doi.org/10.3390/electronics11040513

Academic Editors: Nima Karimian and Tempestt Neal

Received: 15 January 2022
Accepted: 2 February 2022
Published: 9 February 2022

1. Introduction

Automated identification solutions have become critical for security and privacy in today's digitally linked world [1]. Biometrics is a type of person recognition method; it is a security solution that differs from typical authentication and identification techniques such as passwords, ID cards, and PIN codes [2].

Biometrics are techniques that use automated ways to objectively validate a system utilizing biological features. It uses physiological or behavioral aspects of humans as a means of authenticating personal identity [3]. Physiological characteristics include those retrieved from the human body, such as iris [4], faces [5,6], retinas, veins [7], fingerprints [8–11], palm prints, finger knuckle print, and DNA, ECG [12–15], while behavioral characteristics include voice, stride, signature, and keystroke [16–20]. Biometrics traits are commonly employed in systems such as Security in IoT [21–25], e-banking [26–29], cloud security [30–33], access control [34–37], network security systems [38–42], and ID cards [43–47], and other applications related to IoT [48–52].

Hand-based authentication systems are models that recognize fingerprints [53–57], palm prints, hand geometry, hand form, and hand veins [58,59]. For a long time, hand-based systems have been in the limelight [60]. The success of the systems is due to the trustworthy qualities that give stability, acceptance, simplicity, and robustness [61]. Many corporations, industries, and government agencies now rely on hand-based technology for a variety of purposes, including security [62].

Recently, it was discovered that the finger-knuckle (FKP) [63] is also a biometric element that may be employed in a safe authentication system [64]. It is a hand-based characteristic in which images include information about an individual's finger knuckle lines and textures, which may become a unique anatomical feature and be used to identify a person. These characteristics were proposed and examined in order to overcome some of the limits and shortcomings of earlier hand-based technologies [65], as well as the inconsistencies of the low-cost [2] and small-size imaging equipment used to capture the structure [66]. Local feature extraction is performed on the FKP system, followed by a mixture of local and global feature extractions, geometric feature extraction, and ultimately an enhanced acquisition device that includes both major and minor intrinsic features [11,67–70].

Fingerprint, palm print, hand geometry, and hand vein are examples of biometrics that have been thoroughly investigated [71]. FKP can be regarded as a different biometric identifying technology because of its uniqueness [72]. The following are the FKP's distinct benefits over other biometrics: the surface of FKP is difficult to abrade since individuals normally grasp objects with the inner side of their hands. Because of the non-contact nature of the FKP collection [73], users are more likely to accept it [74]. As such, FKP is regarded as one of the most feasible and effective personal identification technologies in the future [75–79].

The finger knuckle print is a global, one-of-a-kind, and persistent biometric pattern that is utilized for extremely exact personal identification. Recent FKP research has focused on robust feature extraction, contactless/unconstrained acquisition, and fusion techniques [80]. However, the literature includes limited work [81–85].

In order to support corporate, industrial, economic, and social change for competitive advantage of firms and nations, and to improve overall human progress, technological innovation plays an important role in society for satisfying needs, achieving goals, and solving problems of adopters directed to supporting corporate, industrial, economic, and social change [86–90]. Awareness technological and social change requires a thorough understanding of scientific developments and new technological trajectories [91–95].

Biometrics technology as being part of technological innovation [96,97], have received a lot of attention in recent years, especially to current techniques like machine learning and artificial intelligence. As a result of the continual search, contemporary methods known as deep learning were developed [98–100]. These approaches received a lot of interest since they can be used to classify image textures [101–105]. Deep learning is a branch of machine learning research that uses learning algorithms to scan many layers of representation to model complicated relationships in data [106,107]. As a result, high-level traits and ideas have been identified based on the lowest of them. Deep structure refers to the hierarchical structure of features, and most of these models are built on the approach of supervised or unsupervised representation learning. Convolutional architectures are one of the most important tools for deep learning success in image classification. Principal component analysis has recently become one of the most popular deep learning methodologies (PCA) [108]. Deep network training is computationally intensive from the outset and necessitates a large volume of tagged data [109–113].

Feature extraction uses deep learning models (convolution neural networks (CNNs)) strategy, which is employed when there is a lack of training data or resources [54]. It can be done by using a pre-trained model, such as VGG, Inception, SqueezeNet, and ResNet, which have been trained on a large dataset project [114] like ImagNet. VGG CNN is made up of various primary structures, each of which is made up of several linked convolutional layers and full-connected layers. The convolutional kernel has a size of 3 × 3, while the input has a size of 224 × 224 × 3. In general, the number of layers is centered at 16~19 [115]. VGGs have lately demonstrated outstanding performance in many computer vision applications. Many firms, including Adobe, Apple, Facebook, Baidu, Google, IBM, Microsoft, NEC, Netflix, and NVIDIA, have lately employed VGG as one of their deep learning methodologies [80]. As a pre-processing model, (VGG-19 CNN) is utilized. The network depth has been increased as compared to typical convolutional neural networks. It employs an alternating structure of numerous convolutional layers and non-linear activation layers, which outperforms a single convolutional layer. The layer structure may extract image features more effectively, apply Max pooling for down sampling, and alter the linear unit (ReLU) as the activation function, that is, choose the greatest value in the image area as the pooled value of the area. The down sampling layer is primarily used to increase the network's anti-distortion capabilities to the image while keeping the sample's key characteristics and minimizing the number of parameters [116].

This study aims at providing an investigation structure for the use of deep learning in supporting FKP recognition using VGG-19 (f6 and f7); thereof, our study intends to achieve the following objectives:

1. Determine the extent to which deep learning can support FKP recognition using the deep VGG-19 method.
2. Examine the impact of dimensionality reduction on the discriminative power of deep features.
3. Identify the best performing classifier on FKP deep features.
4. Determine the authentication performance when using FKP deep features.

The remainder of the paper is broken into the following sections: The literature review on FKP recognition is presented in Section 2. The methodology used to implement the proposed approach, the dataset used, the performance evaluation measures, and the structure of our experimental model are all shown in Section 3. The experimental model's results are presented and discussed in Section 4. Finally, part 5 depicts the study's findings as well as its future endeavors.

2. Related Work

There has been a lot of study done on FKP recognition for both identification and authentication security, whether for IoT or more general security [116–121]. These are only a few instances.

Lalithamani et al. presented new work in the field of biometric authentication system based on the master finger joint pattern—compared to current systems with simple classifiers such as SVM, PCA, and LDA. Given its accuracy, the deep learning method is best suited for this authentication. The Convolution Neural Network (CNN) extracts features and compares them optimally with trained images. CNN is trained by backpropagation algorithm with random gradient descent and minibatch learning with the help of neural network [7].

Hammouche et al. suggested a novel technique for FKP authentication based on phase congruency with a Gabor Filter bank [122]. Furthermore, Zhang et al. proposed a novel computing framework with the goal of implementing a new efficient feature extraction approach for FKP recognition. The authors conducted a thorough examination of three often utilized local features: local orientation, local phase, and phase congruency. In addition, they developed a method for effectively calculating all characteristics utilizing phase congruency [123]. For an FKP identification system, Muthukumar and Kavipriya used the Gabor feature with an SVM classifier [124].

Heidari and Chalechale presented a unique FKP biometric system in which the feature extraction is a mix of the entropy-based pattern histogram (EPH) and a set of statistical texture characteristics (SSTF). The genetic algorithm (GA) was used to find the best characteristics among the retrieved features. This has been tested on PolyU dataset [73]. While, Singh and Kant developed a multimodal biometric system for person authentication based on FKP and iris characteristics, in which the PCA approach was utilized for feature extraction and the Neuro fuzzy neural network (NFNN) classifier was employed in the identification stage [125].

Chlaoua et al. have developed a simple deep learning method known as principal component analysis. In their proposed approach, PCA has been involved to learn two-stages of filter banks then a simple binary hashing and block histograms for clustering of feature vectors are used. The resultant features are finally fed to the classification step, i.e., linear multiclass Support Vector Machine (SVM). The authors also studied a multimodal biometric system based on matching score level fusion [114].

In Reference [126], a simple CNN end-to-end model is introduced for FKP recognition. The dataset Poly-U FKP is used to evaluate the proposed model and the results gives 99.83% (0.76 and 99.18%, respectively) as the best (standard deviation, mean, respectively) accuracy of recognition. Despite this model being based on a straightforward method for data augmentation with a reduced number of trainable parameters, the latter is composed of a few sets of layers: two connected layers and three convolutional ones. Chalabi et al. also used the PCANet-SVM approach to create a system based on score level fusion of minor and major finger knuckles [62].

Hamidi et al. used two types of pre-trained models, VGG–16 and VGG19, with deep convolutional neural networks to extract features from Finger-Knuckle-Print images in order to construct an efficient multimodal identification system. The results presented in this work reveal that unimodal and multimodal identification systems based on matching score level fusion function extremely well [80].

Fei et al. introduced a new direction convolution difference vector to effectively depict the direction details of finger knuckle images. They then presented a feature learning approach for encoded discriminative direction features for finger knuckle image recognition. The final experimental findings indicate that the proposed method outperforms other Finger knuckle image identification algorithms, demonstrating the usefulness of hash learning-based methods [127].

Many deep learning models have been used for different computer vision tasks. For example, ResNet [128] is a robust model that used an interesting idea of adding the identity block to the CNN architecture in order to make the CNN deeper and reduce the problem of learning degradation in deep CNNs.

Likewise, MobileNet [129] is another interesting CNN which used inverted residual in which the residual connections are created between the bottleneck layers. The small size of this model makes it suitable to be used on mobile devices.

Moreover, ShuffleNet [130] is another CNN model which is suitable for mobile devices. The low computational power of this architecture makes it the right option for many applications. The main reason of this low computational cost is due to two operations used in this CNN, which are channel shuffle and pointwise group convolution.

EfficientNet [131] is a state-of-the-art CNN which introduced exciting ideas to improve the performance of CNNs. EfficientNet suggests that the performance of a CNN can be improved by increasing the depth, number of layers, and the width, number of filters, as well as the resolution of the input image. This architecture has many versions, varying from b0 to b7, each of which has its own depth, width, and resolution scales.

FKP is generally fused with other biometrics to reinforce the intended security system in order to increase the performance of a biometric security system; these approaches include, but are not limited to, the work of [73,132–135].

Despite the large number of FKP recognition methods in the literature [136,137], none are perfect, and each has its own limitations, which are primarily caused by issues inherited from computer vision and machine learning. As a result, there is still room for improvement, especially when using deep learning techniques on FKP images.

3. The Proposed Method

The proposed study aims at investigating the ability of deep features extracted from VGG-19 to improving the performance of FKP biometric recognition.

3.1. Dataset Description

To achieve the objectives of the study, especially as it employs deep learning, we adopt a standard FKP image dataset called IIT Delhi Finger Knuckle Dataset version1.0.20 [138]. The size of this dataset and its diverse FKP images alignment with VGG-19 layered network for deep architecture design. This helps to overcome the limitations associated with acquiescing real-time as this dataset is publicly available for research community. Therefore, our experiment was carried out on IIT Delhi Finger Knuckle Dataset version1.0.20. IIT Delhi Finger Knuckle Dataset contains 790 images for 158 subjects, 5 images each. The size of each image is 80 × 100 pixels. Figure 1 shows sample images of the used dataset.

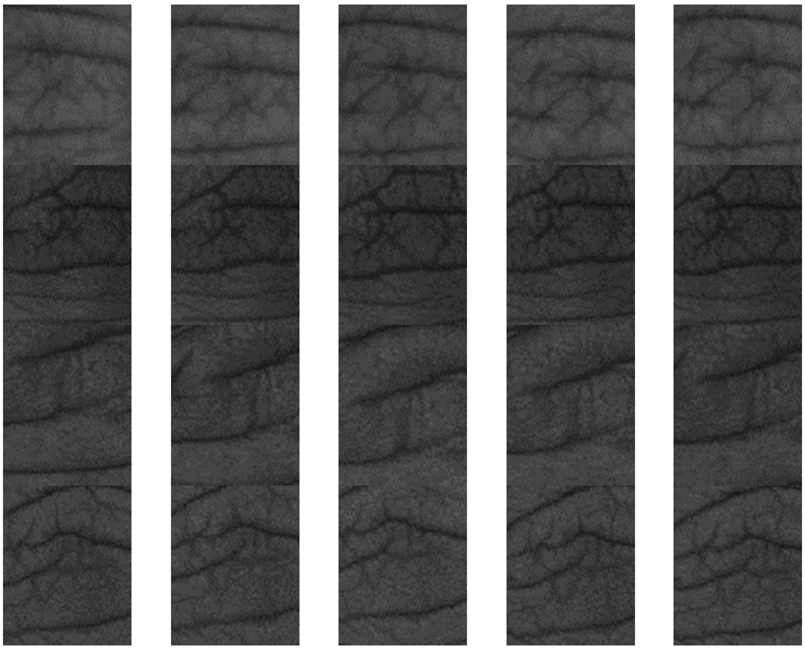

Figure 1. Sample from the IIT Delhi Finger Knuckle Dataset [138].

3.2. The Proposed FKP Recognition

This section presents the proposed framework and procedures for applying the current investigation to obtain the results of using the VGG-19 deep learning-based method for FKP identification or authentication. Figure 2 shows the proposed framework.

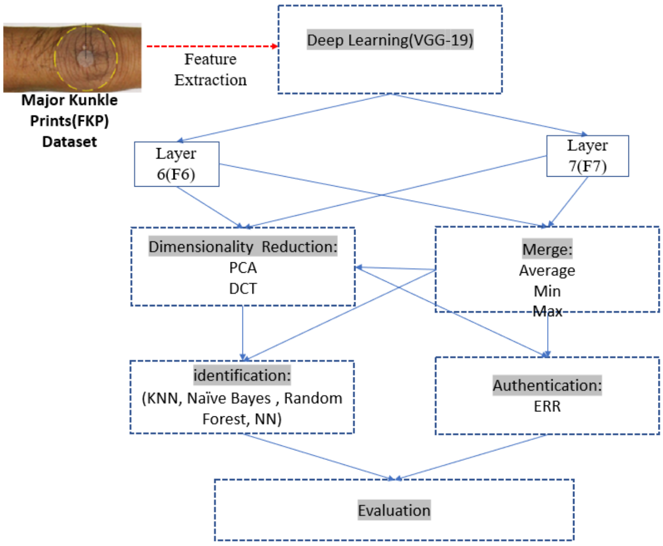

Figure 2. The Proposed FKP recognition Model.

In order to extract features, we used the Pre-trained VGG-19 [139] which was pre-trained on the ImageNet dataset [140]. For feature extraction and training, we used MATLAB 2017a and WEKA tool. We used the Weka tool version (3.6.9) to train and test using the extracted features, and to classify the obtained deep features using some of its supported classification methods, such as ANN, RF, NB, and KNN. All the WEKA methods are used with their default parameters.

MATLAB relies on data format in matrices; so, we use it to run VGG-19 (layers F6 and F7) for feature extraction, and the dimensionality reduction using PCA, in addition to the computation of average, max and min of the deep features merging (discussed later). The output of this phase is two sets of features vectors:

- F6, which is collected from layer 6.
- F7, which is collected from layer 7.

Each set has 790 rows, which are the number of images and examples in the FKP dataset, and 4096 columns, which are the number of features obtained by the pre-trained VGG-19 for each layer. The resultant feature vectors are used for training and testing purposes. F8, on the other hand is a 1000-node classification layer that represents the likelihood of one class in the ImageNet dataset. It is not a common practice to use it here because it does not contain deep features.

After getting the feature vectors, we converted them to an arff file to be compatible with the WEKA tool [48].

The vectors obtained using the pre-trained VGG-19 are very large, 4096 dimensions, therefore, we used WEKA to reduce the number of features. In PCA, the more principal components (PCs) we keep the more dimensionality we get, and vice versa. Therefore, we opt for including all PCs in a manner that retains 95%, 97%, or 99% variance of the data (the 4096 features). Accordingly, we extracted new features sets: PCA99, PCA97, and PCA95, which are reduced versions of the original features. Following this, we used the following classifiers on the new PCA99, PCA97, and PCA95 datasets:

- ANN (Multilayer Perceptron: Weka default parameters: number of hidden layers = (features + classes)/2, learning rate = 0.3).
- RF (Weka default parameters: number of trees in the random forest = 100).
- NB (Weka default parameters: batch size = 100).
- KNN (Weka default parameters: K = 1, linear search with Euclidean distance).

Table 1 shows the number of features after applying the three variance percentages (99%, 97%, and 95%) of PCA to the feature vector of the FKPS datasets (F6 and F7).

Table 1. Number of the features of the training set after the PCA applied.

PCA	Feature Vector	Number of Features
Raw features vector	VGG19F6	4096
	VGG19F7	4096
PCA 99%	VGG19F6	450
	VGG19F7	184
PCA 97%	VGG19F6	271
	VGG19F7	95
PCA 95%	VGG19F6	190
	VGG19F7	68

3.3. Merging F6 and F7

Due to the varying performance of the F6 and F7 features, as will be presented soon, we opt for creating new feature sets by merging both F6 and F7, wishing to obtain deep feature vectors with an improved performance, the merging is done here using any of three methods:

- Minimum:

The minimum merging work by taking the minimum value from each pair of values from F6 and F7. Algorithm 1 explains the minimum merging procedure.

Algorithm 1 Merging of F6 and F7 using minimum method

```
Input: Feature vector F6 and Feature vector F7
Output: Merged feature vector
    Merged feature vector = zeros(length(F6))
    for i = 0 to length(F6))
        $Merged\ feature\ vector_i = min(F6_i, F7_i)$
    end for
    return Merged feature vector
```

- Maximum

The maximum merging works by taking the maximum value from each pair of values from F6 and F7. Algorithm 2 explains the maximum merging procedure.

Algorithm 2 Merging of F6 and F7 using maximum method

```
Input: Feature vector F6 and Feature vector F7
Output: Merged feature vector
    Merged feature vector = zeros(length(F6))
    for i = 0 to length(F6))
        $Merged\ feature\ vector_i = max(F6_i, F7_i)$
    end for
    return Merged feature vector
```

- Average of both F6 and F7:

The average merging works by taking the average value from each pair of values from F6 and F7. Algorithm 3 explains the average merging procedure.

Algorithm 3 Merging of F6 and F7 using average method

```
Input: Feature vector F6 and Feature vector F7
Output: Merged feature vector
    Merged feature vector = zeros(length(F6))
    for i = 0 to length(F6))
        $Merged\ feature\ vector_i = mean(F6_i, F7_i)$
    end for
    return Merged feature vector
```

The three previously mentioned algorithms loop through two feature vectors, F6 and F7. Then each value in the new merged vector is obtained by taking the minimum, maximum, or average of each pair of values. By applying Algorithms 1–3, we get three new deep feature sets; again, we used the dimensionality reduction on these datasets using both PCA. Table 2 shows the number of features after applying PCA with the three variances of data percentages (99%, 97%, and 95%) on the merged feature vectors (F6 and F7), according to average, minimum, and maximum. We call these new deep feature sets MPCA99%, MPCA97%, and MPCA95%.

3.4. Identification and Authentication

The evaluation process of this type of model is done through many different performance measures such as Accuracy, Precision, Recall, and F-score, the values of these measures ranging from 0 to 1, 0 represents the worst performance and 1 represents the best performance. We used 10-Fold cross-validation to verify the reliability of the entered data and validate each method and its recognition ability. In each fold, 79 out of 790 images were tested and 711 images used for training, we mean by "image", the resultant deep feature vector that represents each image.

Table 2. Number of features before and after applying PCA on the merged F6⊕F7.

	Merge Rule	**Number of Features**
Raw features	Min	4096
	Max	4096
	Average	4096
MPCA 99%	Min	557
	Max	583
	Average	431
MPCA 97%	Min	370
	Max	402
	Average	250
MPCA 95%	Min	269
	Max	299
	Average	173

For authentication, five random profiles were chosen, each with five FKP images and a class 1 label. The remaining cases were labeled as class 0. We compared the first profile to all instances in class 0, then profile 2, and so on for all five profiles, using WEKA software. Here we used 5-fold cross validation because we had only 5 images for each subject [141].

4. Results and Discussion

In this section, we present and discuss the experimental results of the proposed framework.

4.1. Experiments Settings

The presented results show the performance of machine learning classifiers on 20 different feature datasets created from the obtained different deep features of the IIT DELHI image dataset. The feature datasets created are listed as follows:

1. The pure F6 feature vector with 4096 dimensions.
2. The pure F7 feature vector with 4096 dimensions.
3. F6 after applying PCA 95%.
4. F6 after applying PCA 97%.
5. F6 after applying PCA 99%.
6. F7 after applying 95%.
7. F7 after applying PCA 97%.
8. F7 after applying PCA 99%.
9. Average feature vector (F6⊕F7).
10. Minimum feature vector (F6⊕F7).
11. Maximum feature vector (F6⊕F7).
12. Average feature vector (F6⊕F7) after applying PCA 95%.
13. Average feature vector (F6⊕F7) after applying PCA 97%.
14. Average feature vector (F6⊕F7) after applying PCA 99%.
15. Minimum feature vector (F6⊕F7) after applying PCA 95%.
16. Minimum feature vector (F6⊕F7) after applying PCA 97%.
17. Minimum feature vector (F6⊕F7) after applying PCA 99%.
18. Maximum feature vector (F6⊕F7) after applying PCA 95%.
19. Maximum feature vector (F6⊕F7) after applying PCA 97%.
20. Maximum feature vector (F6⊕F7) after applying PCA 99%.

The following tables demonstrate the performance metrics for different classifiers while using the above-designed feature vectors.

As shown in Table 3, the identification results of applying VGG-19(F6) on the IIT DELHI dataset show that the KNN achieves the highest accuracy with (81.5%); followed by the RF with (73.4%). While the lowest accuracy was achieved by NB with (68.6%). As for time, KNN spends less time to conduct the training and testing phases with (0.02 s);

while RF spends the maximum time to accomplish the task of predicting with (1.8 s), the training time of the KNN classifier is always zero because it has no training model, each test example is compared directly to the other examples in the training set, this is one reason why KNN is slow in testing, particularly when we have a large number of examples in the training set [142–145].

Table 3. Identification results of VGG-19-F6 deep features. Bold values signify the best performance.

Classifier	Accuracy	Precision	Recall	F-Measure	Training Time (seconds)
KNN	**0.815**	**0.815**	**0.814**	**0.814**	0
RF	0.734	0.725	0.735	0.730	1.8
NB	0.686	0.686	0.717	0.701	1.2

As shown in Table 4, the identification results of applying VGG-19(F7) on the IIT DELHI dataset show that the KNN achieves the highest accuracy with (72.8%); followed by the RF with (69.2%). While the lowest accuracy was achieved by NB with (60.08%). For both F6 and F7, the KNN with acceptable accuracy outperformed all other classifiers. Figure 3 illustrates the accuracy of identification using VGG-19-F6 and VGG-19-F7 deep features, showing that F6 is better for identification regardless of the classifier employed.

Table 4. Identification results of VGG-19-F7 deep features. Bold values signify the best performance.

Classifier	Accuracy	Precision	Recall	F-Measure	Training Time (seconds)
KNN	**0.728**	**0.727**	**0.736**	**0.731**	0
RF	0.692	0.692	0.679	0.685	1.52
NB	0.608	0.646	0.666	0.656	1.16

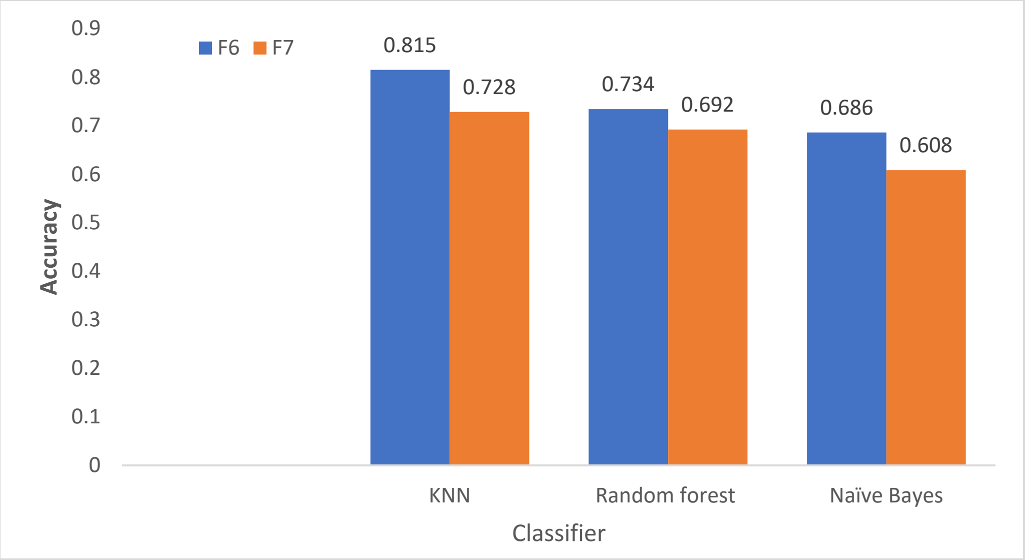

Figure 3. Classifier identification accuracy on each of F6 and F7 deep features. Accuracy results obtained from Tables 3 and 4.

4.2. Results of PCA Features

When PCA is applied to the F6 feature vectors, we get a new set of feature vectors with fewer dimensions. The number of features is determined by the proportion of data variance maintained, the higher the data variance, the more features we use. The new dataset is used then as an input to the classification process.

Table 5 shows the results of the PCA on F6 in terms of identification. We utilize PCA to minimize the feature vector while preserving the highest data variance (95%, 97%, and 99%).

The results of different principal components in Table 5 demonstrate that all classifiers performance have significantly improved in terms of time.

Table 5. Identification results of VGG-19-F6 deep features with PCA (95%, 97%, and 99%). Bold values signify the best performance.

Classifier		Accuracy	Precision	Recall	F-Measure	Training Time (seconds)
PCA 95%	ANN	**0.900**	**0.900**	**0.900**	**0.900**	474.07
	KNN	0.686	0.741	0.766	0.753	0
	NB	0.262	0.382	0.443	0.410	**0.09**
	RF	0.425	0.475	0.490	0.483	1.45
PCA 97%	ANN	**0.886**	**0.886**	**0.885**	**0.885**	410.14
	KNN	0.530	0.671	0.708	0.689	0
	NB	0.276	0.404	0.460	0.431	**0.05**
	RF	0.624	0.631	0.647	0.639	1.72
PCA 99%	ANN	**0.781**	**0.786**	**0.794**	**0.790**	422.58
	KNN	0.512	0.529	0.587	0.557	0
	NB	0.013	0.026	0.080	0.039	**0.03**
	RF	0.495	0.485	0.499	0.492	0.99

Table 5 shows that all classifiers achieve low training time, especially for RF and NB; this is due to the dimensionality reduction achieved by the PCA. The highest accuracy resultant from applying PCA of all percentage of data variance used (95%, 97%, and 99%) is in favor of ANN with (90%, 88.6%, and 78.1%) respectively, which can be attributed to the reduced feature vector by the PCA, which removed redundant features since keeping at least 95% of data variance. However, ANN consumed the highest training time in this experiment, it is worth mentioning that we could not use the ANN classifier with raw features because of its unacceptable training time (days), this is another advantage of dimensionality reduction since it allows for faster training and hence more classifiers to be used.

Similarly, we applied PCA of 95%, 97%, 99% on F7 as well, Table 6 shows the identification results.

Table 6. Identification results of VGG-19-F7 deep features with PCA (95%, 97%, and 99%). Bold values signify the best performance.

Classifier		Accuracy	Precision	Recall	F Measures	Training Time (seconds)
PCA 95%	ANN	**0.849**	**0.848**	**0.853**	**0.850**	205.33
	KNN	0.690	0.608	0.613	0.611	0
	NB	0.442	0.552	0.575	0.564	**0.03**
	RF	0.633	0.629	0.638	0.634	0.92
PCA 97%	ANN	**0.873**	**0.873**	**0.872**	**0.872**	200.39
	KNN	0.714	0.714	0.768	0.740	0
	NB	0.410	0.499	0.536	0.517	**0.02**
	RF	0.629	0.619	0.628	0.623	0.84
PCA99%	ANN	**0.894**	**0.894**	**0.892**	**0.893**	193.26
	KNN	0.677	0.677	0.759	0.716	0
	NB	0.275	0.275	0.437	0.337	**0.02**
	RF	0.559	0.542	0.553	0.548	0.84

Table 6 shows that all classifiers improved in terms of training time, if compared to the F6, which is due to the reduced number of features acquired after applying PCA on layer F7 compared to layer F6 (see Table 1), which may be justified by the nature of the deep features collected at layer F7 of the VGG-19. Moreover, the performance of some classifiers, namely NB and RF have improved in terms of accuracy in most cases. Again, the highest accuracy resultant from applying PCA of (95%, 97%, and 99%) are in favor of ANN with (84.9%, 87.3%, and 89.4%) respectively. However, ANN consumes more training time compared to the other classifiers.

In summary, it can be said that KNN achieves the best results given all performances measures except these of ANN. ANN significantly outperforms all the other classifiers in terms of Accuracy, Precision, Recall, and F-measures.

4.3. Results after Merging F6 and F7

Both deep features (F6, F7) are merged by setting the average, maximum, and minimum as merging rules to evaluate the identification of the FKP using KNN, NB, and RF classifiers. Table 7 shows the identification results.

Table 7. Identification results of VGG-19-deep features obtained by averaging (F6 and F7). Bold values signify the best performance.

Classifier	Accuracy	Precision	Recall	F-Measure	Training Time (seconds)
KNN	**0.806**	**0.806**	**0.803**	**0.805**	0
NB	0.690	0.690	0.720	0.705	0.95
RF	0.729	0.729	0.717	0.723	1.44

Table 7 shows the identification results of the merged dataset based on averaging F6 and F7, in which KNN has the highest accuracy (80.6%), followed by RF and then by the NB with the lowest accuracy.

Table 8 shows the identification result based on maximizing F6 and F7, where KNN has achieved the highest accuracy of (80.3%). On the other hand, the NB has obtained a low accuracy of (67.7%), and the highest training running time is recorded by the RF (1.4 s).

Table 8. Identification results of VGG-19-deep features obtained by maximizing (F6 and F7). Bold values signify the best performance.

Classifier	Accuracy	Precision	Recall	F-Measure	Training Time (seconds)
KNN	**0.803**	**0.803**	**0.800**	**0.801**	0.0
NB	0.677	0.677	0.716	0.696	1.14
RF	0.709	0.718	0.725	0.721	1.4

In Table 9, we can see the identification results based on minimizing F6 and F7, where KNN obtained the highest accuracy (77.8%). On the other hand, the NB obtained the lowest accuracy with (64.7%), and the RF performance was in between.

Table 9. Identification results of VGG-19-deep features obtained by minimizing (F6 and F7). Bold values signify the best performance.

Classifier	Accuracy	Precision	Recall	F-Measure	Training Time (seconds)
KNN	**0.778**	**0.778**	**0.773**	**0.775**	0.0
NB	0.647	0.691	0.710	0.700	0.94
RF	0.697	0.691	0.699	0.695	1.4

Afterwards, we applied the PCA with (95%, 97%, and 99%) on the merged dataset for each resultant feature vectors, Maximum, Minimum, and Average. The results are shown in Tables 10–12.

As can be seen in Table 10, the ANN classifier achieved the highest accuracy compared to the other classifiers; however, it takes a longer training time.

Similar to the maximum deep features, the minimum deep features show that the ANN achieved the highest accuracy compared to the other classifiers; however, it takes a longer training time as shown in Table 11.

Table 10. Identification results of VGG-19-deep features obtained by maximizing (F6 and F7) after applying PCA. Bold values signify the best performance.

	Classifier	Accuracy	Precision	Recall	F Measure	Training Time (seconds)
(PCA 95%)	ANN	**0.894**	**0.894**	**0.892**	**0.893**	781.2
	KNN	0.624	0.715	0.746	0.730	0
	NB	0.287	0.410	0.466	0.436	1.14
	RF	0.657	0.645	0.660	0.652	**0.14**
(PCA 97%)	ANN	**0.846**	**0.846**	**0.839**	**0.842**	1598.19
	KNN	0.457	0.648	0.690	0.669	0
	NB	0.216	0.343	0.400	0.369	**0.17**
	RF	0.567	0.590	0.602	0.596	1.31
(PCA 99%)	ANN	**0.592**	**0.565**	**0.579**	**0.572**	2249.24
	KNN	0.176	0.505	0.565	0.533	0
	NB	0.109	0.209	0.247	0.226	**0.14**
	RF	0.466	0.439	0.450	0.444	1.63

Table 11. Identification results of VGG-19-deep features obtained by minimizing (F6 and F7) after applying PCA. Bold values signify the best performance.

	Classifier	Accuracy	Precision	Recall	F Measure	Training Time (seconds)
(PCA 95%)	ANN	**0.889**	**0.889**	**0.885**	**0.887**	695.57
	KNN	0.653	0.727	0.754	0.740	0
	NB	0.301	0.423	0.480	0.450	**0.05**
	RF	0.651	0.656	0.666	0.661	1.08
(PCA 97%)	ANN	**0.819**	**0.840**	**0.851**	**0.846**	1054.17
	KNN	0.480	0.664	0.701	0.682	0
	NB	0.220	0.346	0.405	0.373	**0.08**
	RF	0.586	0.586	0.570	0.578	1.09
(PCA 99%)	ANN	**0.547**	**0.508**	**0.516**	**0.512**	2118.81
	KNN	0.196	0.546	0.604	0.574	0
	NB	0.157	0.253	0.299	0.274	**0.14**
	RF	0.481	0.462	0.475	0.469	1.4

Table 12. Identification results of VGG-19-deep features obtained by averaging (F6 and F7) after applying PCA. Bold values signify the best performance.

	Classifier	Accuracy	Precision	Recall	F Measure	Training Time (seconds)
(PCA 95%)	ANN	**0.918**	**0.918**	**0.917**	**0.917**	772.1
	KNN	0.722	0.786	0.805	0.795	0
	NB	0.384	0.485	0.527	0.505	**0.12**
	RF	0.701	0.683	0.695	0.689	1.22
(PCA 97%)	ANN	**0.908**	**0.908**	**0.907**	**0.907**	622.02
	KNN	0.594	0.686	0.721	0.703	0
	NB	0.277	0.396	0.449	0.421	**0.06**
	RF	0.622	0.603	0.616	0.609	1.04
(PCA 99%)	ANN	**0.822**	**0.838**	**0.847**	**0.842**	1368.06
	KNN	0.296	0.568	0.622	0.594	0
	NB	0.128	0.233	0.276	0.252	**0.4**
	RF	0.463	0.451	0.464	0.458	1.85

Again, as stated in Table 12, ANN achieved the highest accuracy level among other classifiers; however, it takes longer training time. However, it is worth noting that the ANN and all the classifiers used are in favor of lower data variance (PCA 95%), particularly when using F6 or merging with F6, perhaps this is due to losing more redundant features. One exception is when using the PCA on F7, where we notice improvement in the classifiers' performance, less redundant data on F7 is perhaps the reason. Table 13 summarizes all of the identification accuracy results.

Table 13. Identification accuracy results summery. Bold values signify the best performance.

Feature Vector	Nuber of Features	ANN	KNN	RF	NB	Reduction Percentage
F6 feature vector with 4096 dimensions.	4096	-	**0.815**	**0.734**	0.686	0%
F7 with F6 feature vector with 4096 dimensions	4096	-	0.728	0.692	0.608	0%
F6 after applying PCA 95%.	190	0.900	0.686	0.425	0.262	95%
F6 after applying PCA 97%.	271	0.886	0.530	0.624	0.276	93%
F6 after applying PCA 99%.	450	0.781	0.512	0.495	0.013	89%
F7 after applying PCA 95%.	**68**	0.849	0.690	0.633	0.442	98%
F7after applying PCA 97%.	95	0.873	0.714	0.619	0.499	98%
F7 after applying PCA 99%.	184	0.894	0.677	0.559	0.275	96%
Average feature vector (F6 + F7).	4096	-	0.806	0.729	**0.690**	0%
Minimum feature vector (F6 + F7)	4096	-	0.778	0.697	0.647	0%
Maximum feature vector (F6 + F7).	4096	-	0.803	0.709	0.677	0%
Average (F6 + F7) PCA 95%.	173	**0.918**	0.722	0.701	0.384	96%
Average (F6 + F7) PCA 97%.	250	0.908	0.594	0.622	0.277	94%
Average feature (F6 + F7) PCA 99%.	431	0.822	0.296	0.463	0.128	89%
Minimum (F6 + F7) PCA 95%.	269	0.889	0.727	0.656	0.423	93%
Minimum (F6 + F7) PCA 97%.	370	0.819	0.480	0.586	0.220	91%
Minimum (F6 + F7) PCA 99%.	557	0.547	0.196	0.481	0.157	86%
Maximum (F6 + F7) PCA 95%.	299	0.894	0.624	0.657	0.287	93%
Maximum (F6 + F7) PCA 97%.	402	0.846	0.457	0.567	0.216	90%
Maximum (F6 + F7) PCA 99%.	583	0.592	0.176	0.466	0.109	86%

Table 14 shows a direct comparison of the proposed method to some of the other methods that used the same database, which include Surrounded Patterns Code (SPC) [146], Enhanced Local Line Binary Pattern (ELLBP) [147], Local Binary Patterns (LBP) [148], Centralized Binary Patterns (CBP) [149], Center-Symmetric Local Binary Pattern (CSLBP) [150], and Local Binary Patterns for Finger Outer Knuckle (LBP-FOK) [151]. Moreover, we compared our method to some of the-state-of-the-art deep learning-based feature extraction methods such as ResNet18 [128], MobileNetV2 [129], ShuffleNet [111], and Efficient-Netb0 [131]. To extract the deep features using these deep learning-based methods, we employed their pre-trained versions. The features are retrieved from the layer immediately preceding the classification layer. The features are then classified using the ANN after PCA 95% is applied.

Table 14. Direct comparison of the proposed method to other methods. Bold values signify the best performance.

Method	Accuracy (%)
Proposed	**91.8**
SPC	54.1
ELLBP	70.47
LBP	71.63
CBP	76.67
CSLBP	76.74
LBP-FOK	85.97
Resnet18	88.48
MobileNetV2	44.85
ShuffleNet	52.28
EfficientNetb0	**92.91**

As presented in Table 14, the proposed method achieves superior results to six hand-crafted methods which are SPC, ELLBP, LBP, CBP, CSLBP, and LBP-FOK. In addition, other deep learning approaches outperformed all hand-crafted methods. Furthermore, the proposed method outperforms MobileNet, ShuffleNet, and Resnet18 when compared to other deep learning methods. EfficientNet, on the other hand, achieved slightly better 1% results than our proposed method.

4.4. Authentication

Knowing that Authentication is different from Identification in biometric systems, in this study, to conduct an authentication experiment, five profiles were randomly chosen, each of which has five FKP images labelled as class 1, belonging to one of the subjects. The rest of the images belonging to the rest of the subjects are labelled as class 0. The resultant image dataset is called profile 1, which is used to authenticate subject 1 using the same approach, for the sake of simplicity, we created five profiles only, each authenticate a specific subject. We then obtained the deep features using the same aforementioned methodology, that is we used F6 and F7 features after applying PCA 95%. For the performance assessment, the 5-fold cross-validation was applied with KNN to obtain the averaged authentication results. Note that the main aim here is to find out the ability of these features to give a unique representation of each subject in the FKP images dataset, and therefore, it can be reliably employed for authentication purposes.

For evaluation purpose, the Equal Error Rate (EER) is considered as a measure for typical biometric systems, it is normally used to predetermine the threshold values based on the false acceptance rate and the false rejection rate in a particular biometric system [152]. Tables 15 and 16 present the Authentication EER based on the data profiles created for the purpose of authentication in this study.

Table 15. Authentication ERR of VGG-19-F6 deep features after applying PCA (95%).

Dataset	**EER %**
Profile 1	0.5
Profile 2	0.12
Profile 3	0.12
Profile 4	0.12
Profile 5	0.37
Avg.	0.24

Table 16. Authentication ERR of VGG-19-F7 deep features after applying PCA (95%).

Experiments	**EER %**
Profile 1	0.1
Profile 2	0.12
Profile 3	0.12
Profile 4	0.63
Profile 5	0.2
Avg.	0.23

As can be seen from Tables 15 and 16, the average authentication for EER is very small (0.24% when using F6-PCA, and 0.23% when using F7-PCA), having such a small error rate means that the accuracy of the authentication system is very high, this is expected since the number of classes in authentication systems is typically two, while in the identification problem it is equal to the number of subjects in the dataset.

Based on the results in Table 17, our proposed approach, which investigates the use of deep learning for FKP authentication, has a low error rate and a high false rejection rate when compared to the other methods such as the work of [153]. However, to the best of our knowledge, very few previous studies tackled the feasibility of deep learning (VGG-19) in the improvement of FKP recognition using ANN, KNN, NB, or RF. However, several studies discussed the feasibility of FKP recognition using machine learning classifiers.

However, as a matter of fact, the lower EER, the more accurate the process is. Therefore, compared to [153]; our proposed approach maintains a lower EER rate in both cases of F6 and F7 using PCA. Similarly, lower EER when compared with EER by [154].

Table 17. Authentication EER of [153] compared to ours. Bold values signify the best performance.

Methodology	EER %
VGG19 F6 + PCA	**0.24**
VGG19 F7 + PCA	**0.23**
[153]	1.02

4.5. Discussion

For the identification/authentication of FKP, our Investigation, which is based on the evidence in hand (the dataset used, and the method used) concludes the following:

- The ANN is the best classifier to be used for deep features extracted using VGG-19, if it is provided with the reduced version of the features, otherwise, i.e., if it is applied on the original pure deep features, which obtained from the VGG-19 layer 6 or 7 or any merging of them both, the training time would be unacceptably long.
- Using the PCA does not only reduce the dimensionality, and therefore, the training time significantly, but also allows for increasing the identification accuracy, particularly when using the ANN classifier.
- In general, the original pure F6 provides more distinctive features compared to F7, this is evident from the first 8 rows in Table 13.
- Merging the deep features from layers 6 and 7 allows for more distinctive features, particularly, when using the averaging rule.
- The dimensionality reduction using PCA on the averaged deep features is the best combination to provide the most distinctive features compared to the other approaches investigated.
- The extracted features from the deep features using PCA with 95% of data variance are more distinctive and smaller in number if compared to the other two percentages (97% and 99%) used, this is evident from the highest accuracy achieved by the ANN classifier on the deep features obtained by averaging (F6+F7) after applying PCA 95%, see Table 13, row 14.
- As for the authentication of FKP our investigation concludes that using deep features obtained from either layer 6 or layer 7 leads to a reasonable FKP authentication system, particularly when applying PCA on these deep features.

5. Conclusions

In this paper, deep learning network VGG-19 is investigated to be used for FKP identification or authentication system, using the deep features collected at layers 6 and 7, with and without dimensionality reduction tools such as the PCA, merging both deep features (F6 and F7) is also investigated using different rules such as average, maximum, and minimum.

For the identification system, several machine learning classifiers were applied (such as ANN, KNN, NB, and RF) on deep features obtained from the open-access dataset IIT Delhi Finger Knuckle Dataset. The experimental results show that the best identification result was obtained when applying the ANN classifier on the principal components of the averaged feature vector of F6 and F7 deep features preserving 95% of the data variance. The results also show the potential of using these deep features for an FKP authentication system.

Furthermore, comparisons to state-of-the-art deep learning-based methods demonstrate the superiority of the proposed solution; however, we discovered that another deep learning feature extraction method, EfficientNet, slightly outperforms ours, hence we recommend more research to be conducted on our method and the other deep features method, perhaps incorporating more than one deep features method for FKP recognition.

Aside from the recognition accuracy, the study's limitations include the use of only one FKP dataset, one Deep learning method (VGG), and one dimensionality reduction method (PCA), which we believe is insufficient to make substantial conclusions. As a result, future research will involve using a more standard FKP dataset with a larger number of images and subjects. Moreover, more deep learning networks will be investigated such as AlexNet [155], GoogleNet [156], etc. Besides, other dimensionality reduction techniques can be used for reducing the dimensionality of the deep features such as DCT, wavelet transform, etc., which need to be examined when applied into the deep neural network itself. Moreover, our future work will focus on merging other biometrics with the FKP such as face, fingerprint, and hand shape altogether, to obtain their deep features in order to provide a more accurate biometric system.

Author Contributions: All authors have contributed equally to this paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable, because the FKP database used is a public and open access image dataset utilized by many researchers. Consent statements obtained by the original authors of the dataset [138].

Data Availability Statement: The dataset used in this paper is publicly available at the dataset website: http://www4.comp.polyu.edu.hk/~csajaykr/IITD/iitd_knuckle.htm, accessed on 13 January 2022.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Angelov, P.P.; Gu, X. Deep rule-based classifier with human-level performance and characteristics. *Inf. Sci.* **2018**, *463*, 196–213. [CrossRef]
2. Trabelsi, S.; Samai, D.; Meraoumia, A.; Bensid, K.; Benlamoudi, A.; Dornaika, F.; Taleb-Ahmed, A. Finger-Knuckle-Print Recognition Using Deep Convolutional Neural Network. In Proceedings of the 2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP), El Oued, Algeria, 15–16 May 2020. [CrossRef]
3. Hassanat, A.B.; Btoush, E.; Abbadi, M.A.; Al-Mahadeen, B.M.; Al-Awadi, M.; Mseidein, K.I.; Almseden, A.M.; Ta-rawneh, A.S.; Alhasanat, M.B.; Prasath, V.S. Victory sign biometrie for terrorists identification: Preliminary results. In Proceedings of the 2017 8th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 4–6 April 2017.
4. Fakroon, M.; Gebali, F.; Mamun, M. Multifactor authentication scheme using physically unclonable functions. *Internet Things* **2020**, *13*, 100343. [CrossRef]
5. Chakraborty, S.; Singh, S.K.; Kumar, K. Facial Biometric System for Recognition Using Extended LGHP Algorithm on Raspberry Pi. *IEEE Sens. J.* **2020**, *20*, 8117–8127. [CrossRef]
6. Elngar, A.A.; Kayed, M. Vehicle Security Systems using Face Recognition based on Internet of Things. *Open Comput. Sci.* **2020**, *10*, 17–29. [CrossRef]
7. Sapkale, M.; Rajbhoj, S.M. A biometric authentication system based on finger vein recognition. In Proceedings of the International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–27 August 2016.
8. Prakash, N.S.; Venkatram, N. Establishing Efficient Security Scheme in Home IOT Devices through Biometric Finger Print Technique. *Indian J. Sci. Technol.* **2016**, *9*, 1–8. [CrossRef]
9. Kanchana, S. Fingerprint Based Biometric Authentication in Iot for Resolving Security Challenges. *Int. J. Res. Anal. Rev.* **2018**, *5*, 1000–1003.
10. Shi, S.; Cui, J.; Zhang, X.-L.; Liu, Y.; Gao, J.-L.; Wang, Y.-J. Fingerprint Recognition Strategies Based on a Fuzzy Commitment for Cloud-Assisted IoT: A Minutiae-Based Sector Coding Approach. *IEEE Access* **2019**, *7*, 44803–44812. [CrossRef]
11. Lalithamani, N.; Balaji, R.; Ramya, M.; Sruthi, S.; Aiswarya, A. Finger Knuckle Biometric Authentication using Convolution Neural Network. *Int. J. Pure Appl. Math.* **2017**, *117*, 31–35.
12. Karimian, N. Cardiovascular PPG biometric key generation for IoT in healthcare domain. In Proceedings of the Mobile Multimedia/Image Processing, Security, and Applications, Baltimore, MD, USA, 13 May 2019. [CrossRef]
13. Zhang, Q. Deep Learning of Electrocardiography Dynamics for Biometric Human Identification in era of IoT. In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication (UEMCON), New York, NY, USA, 8–10 October 2018. [CrossRef]
14. Jiang, X.; Liu, X.; Fan, J.; Ye, X.; Dai, C.; Clancy, E.A.; Farina, D.; Chen, W. Enhancing IoT Security via Cancelable HD-sEMG-Based Biometric Authentication Password, Encoded by Gesture. *IEEE Internet Things J.* **2021**, *8*, 16535–16547. [CrossRef]

15. Barros, A.; Rosario, D.; Resque, P.; Cerqueira, E. Heart of IoT: ECG as biometric sign for authentication and identification. In Proceedings of the 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019, Tangier, Morocco, 24–28 June 2019.
16. Shah, D.; Haradi, V. IoT Based Biometrics Implementation on Raspberry Pi. *Procedia Comput. Sci.* **2016**, *79*, 328–336. [CrossRef]
17. Wazid, M.; Das, A.K.; Bhat, V.K.; Vasilakos, A.V. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *J. Netw. Comput. Appl.* **2020**, *150*, 102496. [CrossRef]
18. Sujarani, R.; Manivannan, D.; Manikandan, R.; Vidhyacharan, B. Lightweight Bio-Chaos Crypt to Enhance the Security of Biometric Images in Internet of Things Applications. *Wirel. Pers. Commun.* **2021**, *119*, 2517–2537. [CrossRef]
19. Subhasini, M.S. Lightweight Biometric System for Internet of Things (IoT) Security. *Int. J. Res. Appl. Sci. Eng. Technol.* **2019**, *7*, 163–169. [CrossRef]
20. Alsahlani, A.Y.F.; Popa, A. LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. *J. Netw. Comput. Appl.* **2021**, *192*, 103177. [CrossRef]
21. Alsellami, B.M.; Deshmukh, P.D. The Recent Trends in Biometric Traits Authentication Based on Internet of Things (IoT). In Proceedings of the International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021, Coimbatore, India, 25–27 March 2021.
22. Hossain, M.S.; Muhammad, G.; Rahman, S.M.M.; Abdul, W.; Alelaiwi, A.; Alamri, A. Toward end-to-end biomet rics-based security for IoT infrastructure. *IEEE Wirel. Commun.* **2016**, *23*, 44–51. [CrossRef]
23. Hassen, O.A.; Abdulhussein, A.A.; Darwish, S.M.; Othman, Z.A.; Tiun, S.; Lotfy, Y.A. Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IOT Blockchain Network. *Symmetry* **2020**, *12*, 1699. [CrossRef]
24. Karimian, N.; Tehranipoor, M.; Woodard, D.; Forte, D. Unlock Your Heart: Next Generation Biometric in Re-source-Constrained Healthcare Systems and IoT. *IEEE Access* **2019**, *7*, 49135–49149. [CrossRef]
25. Vorakulpipat, C.; Takahashi, T.; Rattanalerdnusorn, E.; Thaenkaew, P.; Inoue, D. Usable and Secure Cloud-based Biometric Authentication Solution for IoT Devices. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018. [CrossRef]
26. Lee, A. A comparative study on biometric based authentication method for IOT service. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 1–11.
27. Chauhan, T.; Singh, A. Investigating scope of enhanced biometric security for IOT based Digital Wallet. In Proceedings of the 12th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2021, Bangkok, Thailand, 27–28 August 2021.
28. Spehar, J.; Fuks, A.; Vauclair, M.; Meijer, M.; Van Beek, J.; Shao, B. Power Challenges Caused by IOT Edge Nodes: Securing and Sensing Our World. In Proceedings of the 2019 31st International Symposium on Power Semiconductor Devices and ICs, Shanghai, China, 19–23 May 2019. [CrossRef]
29. Ghazali, T.K.; Zakaria, N.H. Security, comfort, healthcare, and energy saving: A review on biometric factors for smart home environment. *J. Comput.* **2018**, *29*, 189–208.
30. Yang, W.; Wang, S.; Hu, J.; Ibrahim, A.; Zheng, G.; Macedo, M.J.; Johnstone, M.N.; Valli, C. A cancelable iris-and ste-ganography-based user authentication system for the internet of things. *Sensors* **2019**, *19*, 2985. [CrossRef]
31. Srivastava, M. Physiological Biometric an Adequate Security Measure for IoT Applications. In Proceedings of the 2nd International Conference on Advanced Computing and Software Engineering (ICACSE), Sultanpur, Uttar, India, 8–9 February 2019.
32. Nadia, R.; Tama, B.A.; Song, J.S. Seamless Human Impedance-based IoT Authentication with Machine Learning Techniques. In Proceedings of the International Conference on ICT Convergence, Jeju Island, Korea, 21–23 October 2020.
33. Abduljabbar, Z.A.; Jin, H.; Ibrahim, A.; Hussien, Z.A.; Hussain, M.A.; Abbdal, S.H.; Zou, D. Secure biometric image re-trieval in IoT-cloud. In Proceedings of the ICSPCC 2016—IEEE International Conference on Signal Processing, Communications and Computing, Hong Kong, China, 5–8 August 2016.
34. Xue, Q.; Ju, X.; Zhu, H.; Zhu, H.; Li, F.; Zheng, X. A Biometric-Based IoT Device Identity Authentication Scheme. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering. *LNICST* **2019**, *287*, 139–149. [CrossRef]
35. Golec, M.; Gill, S.S.; Bahsoon, R.; Rana, O. BioSec: A Biometric Authentication Framework for Secure and Private Com-munication among Edge Devices in IoT and Industry 4.0. *IEEE Consum. Electron. Mag.* **2020**, *1*, 1–6. [CrossRef]
36. Mandal, S.; Bera, B.; Sutrala, A.K.; Das, A.K.; Choo, K.-K.R.; Park, Y. Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment. *IEEE Internet Things J.* **2020**, *7*, 3184–3197. [CrossRef]
37. Batool, S.; Saqib, N.A.; Khattack, M.K.; Hassan, A. Identification of Remote IoT Users Using Sensor Data Analytics. *Lect. Notes Netw. Syst.* **2020**, *69*, 328–337. [CrossRef]
38. Yang, W.; Wang, S.; Sahri, N.M.; Karie, N.M.; Ahmed, M.; Valli, C. Biometrics for Internet-of-Things Security: A Review. *Sensors* **2021**, *21*, 6163. [CrossRef]
39. Wazid, M.; Das, A.K.; Odelu, V.; Kumar, N.; Conti, M.; Jo, M. Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. *IEEE Internet Things J.* **2017**, *5*, 269–282. [CrossRef]
40. Punithavathi, P.; Geetha, S. Partial DCT-based cancelable biometric authentication with security and privacy preservation for IoT applications. *Multimed. Tools Appl.* **2019**, *78*, 25487–25514. [CrossRef]

41. Ross, A.; Banerjee, S.; Chowdhury, A. Security in smart cities: A brief review of digital forensic schemes for biometric data. *Pattern Recognit. Lett.* **2020**, *138*, 346–354. [CrossRef]
42. Sharma, S.K.; Khuntia, B. Service layer security architecture for iot using biometric authentication and cryptography technique. *Adv. Intell. Syst. Comput.* **2021**, *1171*, 291–301.
43. Srikrishnaswetha, K.; Kumar, S.; Ghai, D. Secured Electronic Voting Machine Using Biometric Technique with Unique Identity Number and IOT. Lecture Notes in Networks and Systems. In *Innovations in Electronics and Communication Engineering*; Springer: Singapore, 2020; Volume 107, pp. 311–326. [CrossRef]
44. Bracciale, L.; Loreti, P.; Pisa, C.; Shahidi, A. Secure Path: Block-Chaining IoT Information for Continuous Authentication in Smart Spaces. *IoT* **2021**, *2*, 326–340. [CrossRef]
45. Goyal, M. Enhancing security in Internet of Things using authentication techniques: A review survey. *J. Phys. Conf. Ser.* **2021**, *2007*, 012023. [CrossRef]
46. Sowjanya, G.; Nagaraju, S. Design and implementation of door access control and security system based on IOT. In Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016, Coimbatore, India, 26–27 August 2016; pp. 1–4.
47. Joshy, A.; Jalaja, M.J. Design and implementation of an IoT based secure biometric authentication system. In Proceedings of the 2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems, SPICES 2017, Kollam, India, 8–10 August 2017; pp. 1–13. [CrossRef]
48. Hassanat, A.B.A. On Identifying Terrorists Using Their Victory Signs. *Data Sci. J.* **2018**, *17*, 27. [CrossRef]
49. Tarawneh, A.S.; Chetverikov, D.; Verma, C.; Hassanat, A.B. Stability and reduction of statistical features for image clas-sification and retrieval: Preliminary results. In Proceedings of the 2018 9th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 3–5 April 2018.
50. Al-Shamaileh, M.Z.; Hassanat, A.B.; Tarawneh, A.S.; Rahman, M.S.; Celik, C.; Jawthari, M. New Online/Offline text-dependent Arabic Handwriting dataset for Writer Authentication and Identification. In Proceedings of the 2019 10th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 11–13 June 2019. [CrossRef]
51. Hassanat, A.; Al-Awadi, M.; Btoush, E.; Btoush, A.A.; Alhasanat, E.; Altarawneh, G. New Mobile Phone and Webcam Hand Images Databases for Personal Authentication and Identification. *Procedia Manuf.* **2015**, *3*, 4060–4067. [CrossRef]
52. Al-Btoush, A.I.; Abbadi, M.A.; Hassanat, A.B.; Tarawneh, A.S.; Hasanat, A.; Prasath, V.B.S. New Features for Eye-Tracking Systems: Preliminary Results. In Proceedings of the2019 10th International Conference on Information and Communication Sys-tems (ICICS), Irbid, Jordan, 11–13 June 2019.
53. Lee, S.; Jang, S.-W.; Kim, D.; Hahn, H.; Kim, G.-Y. A novel fingerprint recovery scheme using deep neural network-based learning. *Multimed. Tools Appl.* **2021**, *80*, 34121–34135. [CrossRef]
54. Impedovo, D.; Dentamaro, V.; Abbattista, G.; Gattulli, V.; Pirlo, G. A comparative study of shallow learning and deep transfer learning techniques for accurate fingerprints vitality detection. *Pattern Recognit. Lett.* **2021**, *151*, 11–18. [CrossRef]
55. Nogay, H.S. Comparative Experimental Investigation of Deep Convolutional Neural Networks for Latent Fingerprint Pattern Classification. *Trait. Signal* **2021**, *38*, 1319–1326. [CrossRef]
56. Zhong, C.; Xu, P.; Zhu, L. A deep convolutional generative adversarial network-based fake fingerprint generation method. In Proceedings of the 2021 IEEE International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI), Fuzhou, China, 24–26 September 2021. [CrossRef]
57. Zeng, L.; Al-Rifai, M.; Nolting, M.; Nejd, W. Triplet Loss for Effective Deployment of Deep Learning Based Driver Identification Models. In Proceedings of the 2021 IEEE International Intelligent Transportation Systems Conference (ITSC), Indianapolis, IN, USA, 19–22 June 2021.
58. Tarawneh, A.S.; Chetverikov, D.; Hassanat, A.B. A Pilot Comparative Study of Different Deep Features for Palmprint Identification in Low-Quality Images. In Proceedings of the Ninth Hungarian Conference on Computer Graphics and Geometry, Budapest, Hungary, 10 March 2018.
59. Chawla, B.; Tyagi, S.; Jain, R.; Talegaonkar, A.; Srivastava, S. Finger Vein Recognition Using Deep Learning. In Proceedings of the International Conference on Artificial Intelligence and Applications, Singapore, 20–22 October 2021; Springer: Berlin/Heidelberg, Germany, 2021.
60. Bhaskar, B.; Veluchamy, S. Hand based multibiometric authentication using local feature extraction. In Proceedings of the 2014 Interna-tional Conference on Recent Trends in Information Technology, Chennai, India, 10–12 April 2014.
61. Aftab, A.; Khan, F.A.; Khan, M.K.; Abbas, H. Hand-based multibiometric systems: State-of-the-art and future challenges. *PeerJ Comput. Sci.* **2021**, *7*, e707. [CrossRef]
62. Chalabi, N.E.; Attia, A.; Bouziane, A. Multimodal finger dorsal knuckle major and minor print recognition system based on PCANET deep learning. *ICTACT J. Image Video Process* **2020**, *10*, 2153–2158.
63. Woodard, D.L.; Flynn, P.J. Finger surface as a biometric identifier. *Comput. Vis. Image Underst.* **2005**, *100*, 357–384. [CrossRef]
64. Cheng, K.H.; Kumar, A. Contactless biometric identification using 3D finger knuckle patterns. *IEEE Trans. Pattern Anal. Mach. Intell.* **2019**, *42*, 1868–1883. [CrossRef]
65. Duta, N. A survey of biometric technology based on hand shape. *Pattern Recognit.* **2009**, *42*, 2797–2806. [CrossRef]
66. Jaswal, G.; Kaul, A.; Nath, R. Knuckle Print Biometrics and Fusion Schemes–Overview, Challenges, and Solutions. *ACM Comput. Surv.* **2016**, *49*, 1–46. [CrossRef]

67. Obaidat, M.S.; Rana, S.P.; Maitra, T.; Giri, D.; Dutta, S. Biometric security and internet of things (IOT). In *Biometric-Based Physical and Cybersecurity Systems*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 477–509.
68. Gagandeep; Arora, J.; Kumar, R. Biometric Fingerprint Attendance System: An Internet of Things Application. *Lect. Notes Netw. Syst.* **2019**, *32*, 523–530. [CrossRef]
69. Srianusha, K.; Saddamhussain, S.K.; Kumar, K.P. Biometric car security and monitoring system using IOT. In Proceedings of the International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019, Vellore, India, 30–31 March 2019.
70. Meena, G.; Choudhary, S. Biometric authentication in internet of things: A conceptual view. *J. Stat. Manag. Syst.* **2019**, *22*, 643–652. [CrossRef]
71. Hassanat, A.B.; Prasath, V.S.; Al-Mahadeen, B.M.; Alhasanat, S.M.M. Classification and gender recognition from veiled-faces. *Int. J. Biom.* **2017**, *9*, 347–364. [CrossRef]
72. Zhang, L.; Zhang, L.; Zhang, D.; Zhu, H. Online finger-knuckle-print verification for personal authentication. *Pattern Recognit.* **2010**, *43*, 2560–2571. [CrossRef]
73. Heidari, H.; Chalechale, A. Biometric Authentication Using a Deep Learning Approach Based on Different Level Fusion of Finger Knuckle Print and Fingernail. *Expert Syst. Appl.* **2021**, *191*, 116278. [CrossRef]
74. Kumar, A.; Ravikanth, C. Personal authentication using finger knuckle surface. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 98–110. [CrossRef]
75. Zhai, Y.; Cao, H.; Cao, L.; Ma, H.; Gan, J.; Zeng, J.; Piuri, V.; Scotti, F.; Deng, W.; Zhi, Y. A novel finger-knuckle-print recognition based on batch-normalized CNN. In Proceedings of the Hinese Conference on Biometric Recognition, Urumqi, China, 11–12 August 2018; Springer: Cham, Switzerland.
76. Liang, Y.; Samtani, S.; Guo, B.; Yu, Z. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet Things J.* **2020**, *7*, 9128–9143. [CrossRef]
77. Tait, B.L. Aspects of Biometric Security in Internet of Things Devices. Advanced Sciences and Technologies for Security Applications. In *Digital Forensic Investigation of Internet of Things (IoT) Devices*; Springer: Cham, Switzerland, 2021; pp. 169–186.
78. Shalaby, A.; Gad, R.; Hemdan, E.E.D.; El-Fishawy, N. An efficient multi-factor authentication scheme based CNNs for securing ATMs over cognitive-IoT. *Peer J Comput. Sci.* **2021**, *7*, e381. [CrossRef]
79. Menaga, S.; Paruvathavardhini, J.; Pragaspathy, S.; Dhanapal, R.; Immanuel, D.J. An efficient biometric based authenticated geographic opportunistic routing for IoT applications using secure wireless sensor network. *Mater. Today Proc.* 2021; *in press*. [CrossRef]
80. Hamidi, A.; Khemgani, S.; Bensid, K. Transfer Learning Using VGG Based on Deep Convolutional Neural Network for Finger-Knuckle-Print Recognition. In Proceedings of the 2nd International Conference on Computer Science's Complex Systems and their Applications, Oum El Bouaghi, Algeria, 25–26 May 2021.
81. Verma, S.K.; Dutta, M. Finger-Knuckle-Print Based Recognition System using LBP and SURF. *Int. J. Comput. Sci. Inf. Technol.* **2015**, *5*, 2863–2867.
82. Prarthana, R.J.; Dhanzil, A.; Mahesh, N.; Raghul, S. An Automated Garage Door and Security Management System (A dual control system with VPN IoT & Biometric Database). In Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018, Coimbatore, India, 29–31 March 2018. [CrossRef]
83. Hamidi, H. An approach to develop the smart health using Internet of Things and authentication based on biometric tech-nology. *Future Gener. Comput. Syst.* **2019**, *91*, 434–449. [CrossRef]
84. Li, X.; Niu, J.; Kumari, S.; Wu, F.; Sangaiah, A.K.; Choo, K.-K.R. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *J. Netw. Comput. Appl.* **2017**, *103*, 194–204. [CrossRef]
85. Savitha, M.; Senthilkumar, M. A unique secure multimodal biometrics-based user authenticated key exchange protocol for generic HIoT networks. *Int. J. Emerg. Trends Eng. Res.* **2020**, *8*, 1610–1619.
86. Coccia, M. Technological Innovation. In *The Blackwell Encyclopedia of Sociology*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2021; pp. 299–317.
87. Coccia, M. Sources of technological innovation: Radical and incremental innovation problem-driven to support competitive advantage of firms. *Technol. Anal. Strat. Manag.* **2016**, *29*, 1048–1061. [CrossRef]
88. Coccia, M.; Finardi, U. New technological trajectories of non-thermal plasma technology in medicine. *Int. J. Biomed. Eng. Technol.* **2013**, *11*, 337. [CrossRef]
89. Coccia, M. Multiple working hypotheses for technology analysis. *J. Econ. Bibliogr.* **2020**, *7*, 111–126.
90. Coccia, M.; Finardi, U. Emerging nanotechnological research for future pathways of biomedicine. *Int. J. Biomed. Nanosci. Nanotechnol.* **2012**, *2*, 299. [CrossRef]
91. Coccia, M. Varieties of capitalism's theory of innovation and a conceptual integration with leadership-oriented executives: The relation between typologies of executive, technological and socioeconomic performances. *Int. J. Public Sect. Perform. Manag.* **2017**, *3*, 148–168. [CrossRef]
92. Coccia, M. Spatial relation between geo-climate zones and technological outputs to explain the evolution of technology. *Int. J. Transit. Innov. Syst.* **2015**, *4*, 5–21. [CrossRef]
93. Coccia, M.; Roshani, S.; Mosleh, M. Scientific Developments and New Technological Trajectories in Sensor Research. *Sensors* **2021**, *21*, 7803. [CrossRef] [PubMed]

94. Coccia, M.; Wang, L. Path-breaking directions of nanotechnology-based chemotherapy and molecular cancer therapy. *Technol. Forecast. Soc. Chang.* **2015**, *94*, 155–169. [CrossRef]
95. Coccia, M. Comparative Hypotheses for Technology Analysis. In *Global Encyclopedia of Public Administration, Public Policy, and, Governance*; Farazmand, A., Ed.; Springer: Cham, Switzerland, 2020.
96. Coccia, M. Disruptive firms and industrial change. *J. Econ. Soc. Thought* **2017**, *4*, 437–450.
97. Coccia, M. A theory of classification and evolution of technologies within a Generalised Darwinism. *Technol. Anal. Strat. Manag.* **2018**, *31*, 517–531. [CrossRef]
98. Tarawneh, A.S.; Hassanat, A.B.; Celik, C.; Chetverikov, D.; Rahman, M.S.; Verma, C. Deep face image retrieval: A comparative study with dictionary learning. In Proceedings of the 2019 10th International Conference on Information and Communication Systems (ICICS), Ibrid, Jordan, 11–13 June 2019.
99. Angelov, P.; Gu, X. MICE: Multi-layer multi-model images classifier ensemble. In Proceedings of the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, 21–23 June 2017.
100. Hassanat, A.; Prasath, V.; Mseidein, K.; Al-Awadi, M.; Hammouri, A. A hybrid wavelet-shearlet approach to robust digital image watermarking. *Informatica* **2017**, *41*, 3–24.
101. Hassanat, A.; Jassim, S. Color-based lip localization method. In Proceedings of the SPIE—The International Society for Optical Engineering, Orlando, FL, USA, 28 April 2010.
102. Hassanat, A.B.; Alkasassbeh, M.; Al-Awadi, M.; Alhasanat, E.A. Color-based object segmentation method using artificial neural network. *Simul. Model. Pract. Theory* **2016**, *64*, 3–17. [CrossRef]
103. Narloch, P.; Hassanat, A.; Altarawneh, A.S.A.; Anysz, H.; Kotowski, J.; Almohammadi, K. Predicting Compressive Strength of Cement-Stabilized Rammed Earth Based on SEM Images Using Computer Vision and Deep Learning. *Appl. Sci.* **2019**, *9*, 5131. [CrossRef]
104. Hassanat, A.; Prasath, V.B.S.; Alkasassbeh, M.; Altarawneh, A.S.A.; Al-Shamailh, A.J. Magnetic energy-based feature extraction for low-quality fingerprint images. *Signal Image Video Process.* **2018**, *12*, 1471–1478. [CrossRef]
105. Hassanat, A.; Alkasassbeh, M.; Al-Awadi, M.; Alhasanat, E. Colour-based lips segmentation method using artificial neural networks. In Proceedings of the 2015 6th International Conference on Information and Communication Systems, ICICS 2015, Irbid, Jordan, 7–9 April 2015.
106. Ghazi, M.M.; Ekenel, K.H. A comprehensive analysis of deep learning based representation for face recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Las Vegas, NV, USA, 27–30 June 2016.
107. Anand, V.; Kanhangad, V. Cross-Sensor Pore Detection in High-Resolution Fingerprint Images. *IEEE Sens. J.* **2021**, *22*, 555–564. [CrossRef]
108. Oquab, M.; Bottou, L.; Laptev, I.; Sivic, J. Learning and transferring mid-level image representations using convolutional neural networks. In Proceedings of the IEEE conference on computer vision and pattern recognition, Columbus, OH, USA, 23–28 June 2014.
109. Shin, Y.-H. A Study on the Security Technology of Real-time Biometric Data in IoT Environment. *J. Korea Soc. Comput. Inf.* **2016**, *21*, 85–90. [CrossRef]
110. Farid, F.; Elkhodr, M.; Sabrina, F.; Ahamed, F.; Gide, E. A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services. *Sensors* **2021**, *21*, 552. [CrossRef] [PubMed]
111. Sengupta, S. A Secured Biometric-Based Authentication Scheme in IoT-Based Patient Monitoring System. *Adv.-Telligent Syst. Comput.* **2020**, *937*, 501–518.
112. Yu, S.; Park, K.S.; Park, Y. A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment. *Sensors* **2019**, *19*, 3598. [CrossRef] [PubMed]
113. Banerjee, S.; Odelu, V.; Das, A.K.; Srinivas, J.; Kumar, N.; Chattopadhyay, S.; Choo, K.-K.R. A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment. *IEEE Internet Things J.* **2019**, *6*, 8739–8752. [CrossRef]
114. Chlaoua, R.; Meraoumia, A.; Aiadi, K.E.; Korichi, M. Deep learning for finger-knuckle-print identification system based on PCANet and SVM classifier. *Evol. Syst.* **2018**, *10*, 261–272. [CrossRef]
115. Luo, H.; Yang, Y.; Tong, B.; Wu, F.; Fan, B. Traffic sign recognition using a multi-task convolutional neural network. *IEEE Trans. Intell. Transp. Syst.* **2017**, *19*, 1100–1111. [CrossRef]
116. Xiao, J.; Wang, J.; Cao, S.; Li, B. Application of a Novel and Improved VGG-19 Network in the Detection of Workers Wearing Masks. *J. Phys. Conf. Ser.* **2020**, *1518*, 012041. [CrossRef]
117. Yang, W.; Wang, S.; Zheng, G.; Yang, J.; Valli, C. A Privacy-Preserving Lightweight Biometric System for Internet of Things Security. *IEEE Commun. Mag.* **2019**, *57*, 84–89. [CrossRef]
118. Rao, M.K.; Santhi, S.G. A Multi-factor Biometric-Based User Authentication Protocol for IoT Networks. *Lect. Notes Netw. Syst.* **2020**, *119*, 125–131. [CrossRef]
119. Parei, A.; Hamidi, H. A method for FIDO management through biometric technology in IOT. *Iran. J. Inf. Process. Manag.* **2018**, *33*, 803–856.
120. Vijay, M.; Indumathi, G. A highly secure Multi- Factor authentication system using biometrics to enhance privacy in Internet of Things (IOT). *Int. Res. J. Multidiscip. Technovation* **2019**, *1*, 26–34. [CrossRef]
121. Taheri, S.; Yuan, J.-S. A Cross-Layer Biometric Recognition System for Mobile IoT Devices. *Electronics* **2018**, *7*, 26. [CrossRef]

122. Hammouche, R.; Attia, A.; Akrouf, S. A novel system based on phase congruency and gabor-filter bank for finger knuckle pattern authentication. *ICTACT J. Image Video Process* **2020**, *10*, 2125–2131.
123. Zhang, L.; Zhang, L.; Zhang, D.; Guo, Z. Phase congruency induced local features for finger-knuckle-print recognition. *Pattern Recognit.* **2012**, *45*, 2522–2531. [CrossRef]
124. Muthukumar, A.; Kavipriya, A. A biometric system based on Gabor feature extraction with SVM classifier for Fin-ger-Knuckle-Print. *Pattern Recognit. Lett.* **2019**, *125*, 150–156. [CrossRef]
125. Singh, S.; Kant, C. FKP and Iris based multimodal biometric system using PCA with NFNN. In Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur, India, 26–28 February 2019.
126. Zohrevand, A.; Imani, Z.; Ezoji, M. Deep Convolutional Neural Network for Finger-knuckle-print Recognition. *Int. J. Eng.* **2021**, *34*, 1684–1693.
127. Fei, L.; Zhang, B.; Teng, S.; Zeng, A.; Tian, C.; Zhang, W. Learning discriminative finger-knuckle-print descriptor. In Proceedings of the ICASSP 2019—2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 12–19 May 2019.
128. Kaiming, H.; Xiangyu, Z.; Shaoqing, R.; Jian, S. Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 27–30 June 2016.
129. Sandler, M.; Howard, A.; Zhu, M.; Zhmoginov, A.; Chen, L.-C. Mobilenetv2: Inverted residuals and linear bottlenecks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018.
130. Zhang, X.; Zhou, X.; Lin, M.; Sun, J. ShuffleNet: An Extremely Efficient Convolutional Neural Network for Mobile Devices. In Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018.
131. Tan, M.; Le, Q. Efficientnet: Rethinking model scaling for convolutional neural networks. In Proceedings of the International Conference on Machine Learning, PMLR, Long Beach, CA, USA, 9–15 June 2019; pp. 6105–6114.
132. Khodadoust, J.; Medina-Pérez, M.A.; Monroy, R.; Khodadoust, A.M.; Mirkamali, S.S. A multibiometric system based on the fusion of fingerprint, finger-vein, and finger-knuckle-print. *Expert Syst. Appl.* **2021**, *176*, 114687. [CrossRef]
133. Jaswal, G.; Poonia, R.C. Selection of optimized features for fusion of palm print and finger knuckle-based person au-thentication. *Expert Syst.* **2021**, *38*, e12523. [CrossRef]
134. Attia, A.; Akhtar, Z.; Chahir, Y. Feature-level fusion of major and minor dorsal finger knuckle patterns for person au-thentication, Signal. *Image Video Process.* **2021**, *15*, 851–859. [CrossRef]
135. Kant, C.; Chaudhary, S. A Multimodal Biometric System Based on Finger Knuckle Print, Fingerprint, and Palmprint Traits. In *Innovations in Computational Intelligence and Computer Vision*; Springer: Singapore, 2021.
136. Fei, L.; Zhang, B.; Tian, C.; Teng, S.; Wen, J. Jointly learning multi-instance hand-based biometric descriptor. *Inf. Sci.* **2021**, *562*, 1–12. [CrossRef]
137. Aizi, K.; Ouslim, M. Score level fusion in multi-biometric identification based on zones of interest. *J. King Saud Univ. Comput. Inf. Sci.* **2019**, *34*, 1498–1509. [CrossRef]
138. Kumar, A.; Zhou, Y. IIT Delhi Finger Knuckle Database (Version 1.0). 2009. Available online: http://www4.comp.polyu.edu.hk/~{}csajaykr/IITD/iitd_knuckle.htm (accessed on 6 January 2022).
139. Simonyan, K.; Zisserman, A. Very deep convolutional networks for large-scale image recognition. In Proceedings of the International Conference on Learning Representations ICLR, San Diego, CA, USA, 7–9 May 2015.
140. Deng, J.; Dong, W.; Socher, R.; Li, L.-J.; Li, K.; Fei-Fei, L. Imagenet: A large-scale hierarchical image database. In Proceedings of the 2009 IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, 20–25 June 2009.
141. Hassanat, A.B.; Tarawneh, A.S.; Abed, S.S.; Altarawneh, G.A.; Alrashidi, M.; Alghamdi, M. RDPVR: Random Data Partitioning with Voting Rule for Machine Learning from Class-Imbalanced Datasets. *Electronics* **2022**, *11*, 228. [CrossRef]
142. Hassanat, A. Furthest-Pair-Based Binary Search Tree for Speeding Big Data Classification Using K-Nearest Neighbors. *Big Data* **2018**, *6*, 225–235. [CrossRef]
143. Hassanat, A.B.A. Two-point-based binary search trees for accelerating big data classification using KNN. *PLoS ONE* **2018**, *13*, e0207772. [CrossRef]
144. Hassanat, A.B.A. Norm-Based Binary Search Trees for Speeding Up KNN Big Data Classification. *Computers* **2018**, *7*, 54. [CrossRef]
145. Hassanat, A.B.A. Furthest-Pair-Based Decision Trees: Experimental Results on Big Data Classification. *Information* **2018**, *9*, 284. [CrossRef]
146. Al-Nima, R.R.O.; Al-Kaltakchi, M.T.; Al-Sumaidaee, S.; Dlay, S.S.; Woo, W.L.; Han, T.; Chambers, J.A. Personal verification based on multi-spectral finger texture lighting images. *IET Signal Process.* **2018**, *12*, 1154–1164. [CrossRef]
147. Al-Nima, R.R.O.; Han, T.; Chen, T.; Dlay, S.S.; Chambers, J.A. Finger Texture Biometric Characteristic: A Survey. *arXiv* **2020**, arXiv:2006.04193.
148. Ojala, T.; Pietikäinen, M.; Harwood, D. A comparative study of texture measures with classification based on featured distributions. *Pattern Recognit.* **1996**, *29*, 51–59. [CrossRef]
149. Fu, X.; Wei, W. Centralized Binary Patterns Embedded with Image Euclidean Distance for Facial Expression Recognition. In Proceedings of the 2008 Fourth International Conference on Natural Computation, Jinan, China, 18–20 October 2008. [CrossRef]

150. Heikkilä, M.; Pietikäinen, M.; Schmid, C. Description of Interest Regions with Center-Symmetric Local Binary Patterns. In *Computer Vision, Graphics and Image Processing*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 58–69. [CrossRef]
151. Al-Nima, R.R.O.; Jarjes, M.K.; Kasim, A.W.; Sheet, S.S.M. Human Identification using Local Binary Patterns for Finger Outer Knuckle. In Proceedings of the 2020 IEEE 8th Conference on Systems, Process and Control (ICSPC), Melaka, Malaysia, 11–12 December 2020. [CrossRef]
152. Tripathi, K. A comparative study of biometric technologies with. *Int. J. Comput. Appl.* **2011**, *14*, 10–15.
153. Choras, M.; Kozik, R. Knuckle biometrics based on texture features, In Proceedings of the International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics, Istanbul, Turkey, 22 August 2010.
154. Kim, J.; Oh, K.; Teoh, A.B.-J.; Toh, K.-A. Finger-knuckle-print for identity verification based on difference images. In Proceedings of the IEEE 11th Conference on Industrial Electronics and Applications, Hefei, China, 5–7 June 2016. [CrossRef]
155. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. ImageNet classification with deep convolutional neural networks. *Adv. Neural Inf. Process. Syst.* **2012**, *25*, 1097–1105. [CrossRef]
156. Szegedy, C.; Liu, W.; Jia, Y.; Sermanet, P.; Reed, S.; Anguelov, D.; Erhan, D.; Vanhoucke, V.; Rabinovich, A. Going deeper with convolutions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Boston, MA, USA, 7–12 June 2015.